

Naviam Cloud and Cloud+ Service Description Lot 2b

Document Name	Naviam Cloud and Cloud+ – G-Service Descriptions
Document Type	Service I Guide
Document Number	GCLD-15-Sd-001
Version	01
Version Date	28/01/2025
Document Author	Naviam Technologies Limited
Approved By	Naviam Technologies Limited

Contents

Background.....	4
Naviam Cloud Solution Set	5
Naviam Starter, Premier & Enterprise Feature Table.....	6
Cloud Services Solution Features	7
Production and Non-Production Instances.....	7
Licensing Options.....	7
SCML Platform VS Dedicated Platform	8
Database Platforms.....	9
Email, SMTP, and Push.....	10
Authentication Methods	10
Naviam Cloud Dashboard	10
Optional Services.....	11
MAS Applications, Industry Solutions, Add-Ons, and Tools.....	11
Third-Party Integrations.....	13
Content Distribution Network Timeouts.....	14
Add-On Services.....	14
Backup & Storage Regime	17
Backup Regime by Platform	17
Production Database Backups	17
Non-Production Database Backups (all NPEs)	17
Production Attached Documents Backups	17
Extended Backup Retention Regime.....	18
Patching, Change, Upgrade Regime.....	19
Patching/Upgrade Cycles for MAS and OpenShift Clusters.....	19
Customer MAS Patching/Upgrade Schedule.....	19
Notification.....	20
Prescriptive & Consultative Patch Schedules for OpenShift Clusters.....	20
Planned Downtimes per Activity	21
New Version Release	22
Patching Outage Timings.....	23

iFixes, Hotfixes and LA Fixes.....	23
Security Vulnerability Fixes	23
Service Level Agreement	25
Component Availability	25
Availability Terms.....	26
Naviam Cloud and Cloud+ Standard Solution Set SLA.....	27
Naviam Response Commitment & Product-Specific SLA	27
Naviam Hosted Product SLA.....	27
Service Credits	28
Elements of Service Covered by the Service Credit Scheme	28
99.95% Availability Target	28
99.99% Availability Target	29
Claiming Service Level Credits.....	29
Change Freeze Periods.....	29
Appendix A – Naviam Software Solutions.....	30
Naviam Elevate Suite	30
Data Management for Maximo	30
Naviam Mobile Solutions.....	34
Naviam Datastudio	34
Appendix B – Naviam Mobile Solutions.....	36
Opqo by Naviam	36
EZMaxMobile by Naviam.....	37
Fingertip by Naviam.....	38

Background

References to Naviam: All references to Naviam within this document are inclusive of the Supplier as defined within the Master Services Agreement, as well as Supplier-affiliated companies.

Cross-reference to definitions: Capitalised terms used but not defined in this Naviam Cloud and Cloud+ Service Description shall have the meanings given to them in (i) the Evergreen Glossary of Terms, or (ii) where not defined in the Evergreen Glossary of Terms, the Master Services Agreement (where applicable).

Precedence clause: In the event of any conflict or inconsistency between the terms of the contract documents: (i) this Naviam Cloud and Cloud+ Service Description shall prevail over the Evergreen Glossary of Terms and the MSA in respect of the specific products and services described herein; (ii) the Evergreen Glossary of Terms shall prevail over the MSA (where applicable) in respect of defined terms; and (iii) the MSA (where applicable) shall otherwise prevail over this [Evergreen Document name].

Business Hours & Business Days: Any references to “Business Hours” and/or “Business Days” that are referenced within this document are defined within the Naviam Support Commitment Guide within the Support Time Zones section of the document.

Service Description This document contains details of the Naviam Cloud and Cloud+ offering and services. This serves as a reference guide for Customers and provides information on the standard Naviam Cloud and Cloud+ offerings. The Service Description also details several optional add-on services beyond the standard Cloud and Cloud+ offerings.

Naviam Cloud Solution Set

Naviam offers a standard solution set for the Naviam Cloud and Cloud+ offerings, the Naviam Cloud and Cloud+ standard solution. The below bullet points clarify the meanings of each definition or symbol within the preceding table:

- **✓:** Component is bundled with the offering at no extra fee.
- **Available:** Component can be bundled at no extra fee but must be requested.
- **Implementation Required:** Component is included upon request but requires implementation for additional fees. **Note:** More information on what additional functionality they offer are provided in Appendix **A and B**.
- **Optional Add-On:** Component is not included in the offering, but the component/implementation can be purchased separately. **Note:** More information on what additional functionality they offer are provided in Appendix **A and B**.

Component	Naviam Cloud+	Naviam Cloud
MAS Manage	✓ Licence Included Subscription Offering	✓ Bring Your Own Licence Offering
Cloud Dashboard	✓	✓
Naviam Elevate Suite	✓	✓
Naviam DataStudio	✓	Optional Add-On
Opqo by Naviam	Available	Available - Up to 5 Users Optional - Systems larger than 5 Users
Naviam Accelerators	Available	Available
Fingertip / EZMaxMobile	Implementation Required	Optional Add-On
Naviam GIS	Implementation Required	Optional Add-On
Naviam Vendor	Implementation Required	Optional Add-On
Naviam Planner	Implementation Required	Optional Add-On
Naviam Request	Implementation Required	Optional Add-On

Naviam Starter, Premier & Enterprise Feature Table

Within the Naviam Cloud and Cloud+ standard solution set, the Naviam Starter, Premier, and Enterprise offerings are available. The selection of the offering tier (Starter, Premier, or Enterprise) depends on Customer requirements, specification differences, and fees. Naviam Starter, Premier, and Enterprise are available in the offering tiers outlined within the table below.

Offering Feature	Starter	Premier	Enterprise
Bring Your Own Licence Option	Yes	Yes	Yes
Maximum User Count	50 named and 25 concurrent	Unlimited	Unlimited
OpenShift Clusters (Default)	SCML	SCML (option for Dedicated)	Dedicated
Availability SLA (monthly)	99.95%	99.95%	99.99%
Standard RTO / RPO	72 / 2	24 / 2	16 / 1
Dashboard Cloud Users	2	2 (option for additional)	10 (option for additional)
Database Starting size	50GB	100GB	250GB
Database Maximum size	100GB	Unlimited	Unlimited
Database Increment block size	50GB	100GB	250GB
Doclinks Starting Size	1 TB	3 TB	3 TB
Doclinks Maximum Size	3 TB	No Limit	No Limit
Doclinks Growth Increment Size	1 TB	1 TB	1 TB

Cloud Services Solution Features

This section explains details of specific elements and certain components within the Naviam Cloud and Cloud+ standard solution set.

Production and Non-Production Instances

The Production Environment provided with the Cloud Services serves as the operational instance intended for use in live business operations.

The Non-Production Environment provided with the Cloud Services is a copy of the Production Environment (same build, scaled differently). This is intended to be used for quality assurance testing. Changes must be made within the Non-Production Environment before being made to the Production Environment.

The Naviam Cloud and Cloud+ Solution include a default number of environments to be provisioned as documented in the table below.

	Starter	Premier	Enterprise
Production	1x: 24x7x365	1x: 24x7x365	1x: 24x7x365
Non-Production	0.3 (Option for up to 0.5)	1 (no limit on additional environments)	2 (no limit on additional environments)

Naviam Starter Part-Time NPE

The Naviam Starter offering includes a non-production system that is limited to a standard annual uptime of 30%. Uptime is measured as the number of days the system is online annually. Partial days in which the system is online will count as a full day of uptime.

If additional uptime beyond 30% is required, then an additional 20% of availability can be purchased for a fee, totalling 50% annual uptime.

Licensing Options

Bring Your Own Licence

The Bring Your Own Licence (BYOL) option allows for Cloud Services to be wrapped around MAS licence entitlements that are owned or purchased by the Customer.

The Customer is responsible for maintaining a licence subscription for software updates, where applicable, for the Naviam Cloud solution. BYOL Customers are responsible for the purchase

of additional licenses, providing Naviam with the license file, and providing Naviam with updated license files in cases of license change, expiration, etc.

In the case that the Customer-owned Maximo App Point licence entitlement is designated "reserved", it does not provide OpenShift entitlement and is subject to an additional platform fee, for which Naviam will procure and quote as an element to the standard service fees.

Licence Included Subscription

Provides Cloud Services in addition to Licence-Included Subscriptions, which grant entitlements to MAS, and certain Naviam apps, features, and administrative tools.

SCML Platform VS Dedicated Platform

Secure Common Management Layer (SCML) Platform Products

Secure Common Management Layer (SCML) is a method where OpenShift clusters host multiple systems. This enables cost efficiencies as the fees of overhead services, appliances, and tooling can be split amongst the various Customer systems being hosted on SCML clusters.

Customers with hosted systems on SCML clusters will have certain elements that are always provisioned as a dedicated element to the Customer, without exception. This includes:

- Customer's own instance of Maximo Application Suite Core
- Customer's own instance of Maximo Manage, plus any other application within the suite
- Customer's own database for Maximo Manage, plus any other application within the suite
- Database file storage
- Attached documents (doclinks) file storage
- Security-enhanced Linux namespaces with the OpenShift cluster

Examples of the elements of SCML platforms which are shared between multiple Customer systems include:

- Nodes (masters and workers) which underpin the OpenShift platform
- Load balancers
- Network gateways and other networking appliances
- Firewalls
- Security and vulnerability monitoring toolsets
- Annual penetration tests
- Annual disaster recovery tests
- Performance and capacity monitoring toolsets

While some elements and appliances are shared on an SCML platform, the security and integrity of individual Customer systems are always maintained. SCML platforms allow for

complete data segregation between hosted Customer systems through the provisioning of dedicated MAS core instances, dedicated Maximo Manage instances, and dedicated databases per Customer.

In addition, Maximo Application Suite deploys pods into separate security-enhanced Linux namespaces, which are always dedicated per Customer. Strict ingress and egress rules are also enforced with OpenShift network policies applied to all pods within those namespaces. Naviam also enforces strict role-based access control rules aligned to identity provider groups controlling access to each dedicated namespace.

Dedicated Platform

For Naviam Cloud and Cloud+ systems where the OpenShift clusters are marked as “Dedicated”, then all Naviam-provisioned infrastructure for these systems is dedicated to a single Customer system on the platform, and no elements are shared with any other Customer systems.

Database Platforms

Standard Database Platforms

The standard database platforms for use with Naviam Cloud and Cloud+ systems are Microsoft SQL Standard-Shared and DB2. Naviam Cloud and Cloud+ Starter Customers are required to utilise Microsoft SQL Standard-Shared.

For systems utilising the SQL Standard-Shared platform, the database server time zone will be UTC.

Premium Database Platforms

The premium database platforms available for use with Naviam Cloud and Cloud+ systems are Microsoft SQL Standard-Dedicated and Oracle Standard. Additional fees will apply for Premium Database Platforms. Available to Naviam Cloud and Cloud+ Premier and Enterprise systems.

Enterprise Database Platforms

The Enterprise Database platforms available for use with Naviam Cloud and Cloud+ systems are DB2 Advanced, SQL Enterprise, and Oracle Enterprise. Additional fees will apply for Enterprise Database platforms. Available to Naviam Cloud and Cloud+ Enterprise systems.

Email, SMTP, and Push

There are two methods to enable emails to be sent for the Naviam Cloud and Cloud+ solution:

- Customer-Provided SMTP Service
- Simple Email Service Setup

Due to the nature of messages being delivered across the internet, email delivery and push notifications are provided on a best-effort basis.

Authentication Methods

The setup of SAML (Security Assertion Markup Language) is the standard method included with the Cloud Services. SCIM Authentication is also available as an add-on offering.

SSO (Single Sign On) will no longer be supported by Naviam using LDAP or LDAPS authentication since the inception of Maximo Application Suite.

Native Authentication (using credentials stored inside the Application Layer database) is supported by Naviam and will continue to be for as long as IBM supports it as the vendor of Maximo Application Suite. However, SSO via SAML (/SCIM) provides a level of control and security for Customer IT teams that is preferable to Native Authentication at the Application Layer. Naviam always suggests SSO as the default standard methodology for authentication.

Naviam Cloud Dashboard

The Naviam Cloud Dashboard is available to Naviam Cloud and Cloud+ systems, providing real-time visibility into the application's current health status and key monitoring metrics. The Naviam Cloud Dashboard provides insight into current application status with the ability to drill down into logs and allows Customers to have visibility into Change and Incident records.

Naviam Cloud Dashboard is included, and the Starter and Premier Naviam Cloud and Cloud+ systems will include two Naviam Cloud Dashboard users by default. Naviam Cloud and Cloud+ Enterprise systems include 10 users by default. Additional Dashboard users are available for a fee for Naviam Cloud and Cloud+ Premier and Enterprise systems.

Optional Services

There are several optional services available with the Naviam Cloud and Cloud+ solution. These are applications, industry solutions, add-ons, third-party products, and added services that enable the expanded use of the Naviam Cloud and Cloud+ offerings. At times, optional or additional services may carry additional fees or licensing requirements.

MAS Applications, Industry Solutions, Add-Ons, and Tools

The MAS and Manage applications, industry solutions, add-ons, and tools are available for deployment to MAS and Manage with the Naviam Cloud and Cloud+ offerings. Certain MAS applications, industry solutions, add-ons, and tools may be no-fee to deploy, but others may carry additional fees due to requirements for additional middleware/hosting, licensing, labour, etc. Following the deployment of an industry solution, the Customer may be unable to remove the industry solution from the system.

The MAS applications, industry solutions, add-ons and tools available with the Naviam Cloud and Cloud+ standard solution set are documented within the table below.

Installable: Does not carry additional fee(s) to deploy.

Optional: Carries additional fee(s) to deploy, e.g. licensing, hosting, labour.

Roadmap: Planned for development or in the development process.

	Naviam Starter	Naviam Premier	Naviam Enterprise
MAS Applications			
Manage with Health	Installable	Installable	Installable
Maximo Monitor		Optional	Optional
Maximo Visual Inspection		Optional	Optional
Maximo Real Estate and Facilities		Roadmap	Roadmap
Maximo Collaborate (fka Assist)		Roadmap	Roadmap
Maximo Predict		Roadmap	Roadmap
MAS Industry Solutions, Add-ons, and Tools			
Maximo Visual Inspection Edge		Optional	Optional
Maximo Health and Predict - Utilities		Roadmap	Roadmap
IBM MRO Inventory Optimization		Roadmap	Roadmap
Optimizer		Roadmap	Roadmap
Manage Add-ons			
Reliability Strategies¹	Installable	Installable	Installable

	Naviam Starter	Naviam Premier	Naviam Enterprise
Health, Safety, and Environment	Installable	Installable	Installable
Service Provider	Installable	Installable	Installable
Asset Configuration Manager		Installable	Installable
Maximo IT²		Installable	Installable
Spatial		Optional	Optional
Maximo Connector for SAP Applications		Optional	Optional
Maximo Connector for Oracle Applications		Optional	Optional
Maximo Connector for Workday Applications		Optional	Optional
Maximo Connector for Envizi		Optional	Optional
Manage Industry Solutions			
Nuclear	Installable	Installable	Installable
Oil & Gas	Installable	Installable	Installable
Transportation	Installable	Installable	Installable
Utilities		Installable	Installable
Aviation		Optional	Optional
Civil Infrastructure		Roadmap	Roadmap

Notes

[1] Customers using Reliability Strategies are required to comply with the IBM Maximo Manage – Reliability Strategy Library Service Description. The current version of this document is available with the following link: [Reliability Strategy Library Service Description](#). IBM may change this document at any time by posting a revised version of the document.

[2] A Maximo IT AppPoint is a separate and unique product to a MAS AppPoint. Both MAS AppPoints and Maximo IT AppPoints are a requirement to deploy Maximo IT.

Third-Party Integrations

Maximo Integrations

Naviam allows the use of integrations from Maximo to external systems. Certain integrations may require additional hosted components or labour to deploy.

Integrations are only permitted with the Naviam Starter product if they are HTTPS endpoint integrations connected across the public internet only (no VPNs are applicable or supported with the Naviam Starter product).

If an integration is created, configured and introduced by a third party, then the Customer owns the responsibility for ongoing support and maintenance of that integration.

Solution Compatibility

The solution's compatibility with third-party components is not assured in the future; for example, the Apple App Store may remove support for a mobility application.

Moreover, if any third-party component becomes incompatible with the Cloud Services, then Naviam may no longer support or maintain the component as part of the offering.

Maximo Licensing Implications

Not all external systems connected to Maximo are registering Maximo licence usage that would be required to meet the licensing requirements from IBM. All integrated systems must comply with rules stated at: <https://www.ibm.com/docs/en/masv-and-l/cd?topic=suite-licensing-in-maximo-application-90-earlier> (9.0 and earlier) or <https://www.ibm.com/docs/en/masv-and-l/cd?topic=suite-licensing-in-maximo-application-91> (9.1 and later).

The liability to comply with usage outside of what Naviam can audit falls to the Customer, and the Customer is required to acquire the Maximo licensing for these scenarios from their licence provider.

Content Distribution Network Timeouts

Naviam may use Content Distribution Network (CDN) toolsets in the Cloud Services to speed up website content delivery and user experience, as well as to provide specific web security measures.

Such toolsets may impose a limit on the maximum time allowed to establish a connection, receive data, or complete a request before the message is considered a failure. Customers should note that to succeed within these timeout limits, any connections, data calls or requests being sent to Maximo via any integration path or route should be engineered to connect and succeed within 100 seconds.

Add-On Services

Add-On services allow additional flexibility beyond the standard Naviam Cloud and Cloud+ offerings. The Naviam Add-On services generally carry additional fees or licensing requirements. Add-on services, unless otherwise stated, are not available for use with Naviam Starter.

Additional Non-Production Environment

Provides an NPE or multiple NPEs in addition to the Production Environment(s) and the included Non-Production Environments(s). Additional NPEs are for non-production use, minimally scaled, and are configured to support 25 or fewer concurrent users. Available with Naviam Cloud and Cloud+ Premier or Enterprise systems.

Database Read-Only Replicas

Provides a database read-only replica to Customers. This can be used for database reporting and querying; it does not affect primary database performance. Available with Naviam Cloud and Cloud+ Premier or Enterprise systems.

For SQL Server, Database Read-Only Replicas, SQL Server Enterprise licensing is required. Naviam does include this as an architectural design standard for Naviam Cloud and Cloud+ using SQL Server, but Naviam must be notified of this need during the system design.

Private Link: Secure Connectivity Patterns for DB2 Database Connection

A solution which allows for bi-directional secure database connection using endpoints and load balancers, providing a private connection between the Customer estate and the Naviam-hosted database (s) that are not exposed to the public internet. This can be set up in multiple configurations to match Customer requirements and type of Customer-hosted estate.

Additional Languages

Provides additional language(s) for use within a Naviam Cloud and Cloud+ system. Additional languages are not included with Naviam Cloud and Cloud+ Starter systems, but additional languages are available as an add-on service. Additional Language requests can be completed as part of the included service for Naviam Cloud and Cloud+ Premier and Enterprise systems.

Cross-Region Failover

Provides a failover system that is mirrored in a separate geographical region from the primary hosting geographical region. This allows traffic to redirect to the failover system in the event the primary hosting system unexpectedly goes offline. This is available for Naviam Cloud and Cloud+ systems at the Enterprise offering tier. This is also available to Naviam Cloud and Cloud+ Premier systems that have the Premier Enhanced Hosting Bundle.

Premier Enhanced Hosting Bundle

Provides Naviam Cloud and Cloud+ Premier systems with the option to enhance hosting components to provide a dedicated OpenShift cluster, an improved SLA of 99.99% (inclusive of improved SLA Credits), and an enhanced RTO/RPO of 16/1. Available for Naviam Cloud and Cloud+ Premier systems.

Database Replication using Change Data Capture

A solution that allows the entire database (or part) to be replicated from the Production database using change data capture and stored in an accessible cloud storage location as Parquet files. Such files can then be retrieved by the Customer's chosen data movement and retrieval platform or tool, enabling the Customer to replicate updated change data capture data from the Naviam-hosted system database into the Customer's hosted data repositories or systems.

Weekend Deployments

The weekend deployment service for when cutovers and go-lives cannot be completed on Monday to Friday is available as an included service (upon request) for Naviam Cloud and Cloud+ Enterprise systems. This is not available for Naviam Cloud and Cloud+ Starter or Premier Systems.

Customer Domain Hosting

The use of a customer-owned domain name and certificates for Customer domain hosting on the Maximo webpages is available as an add-on service to Naviam Cloud and Cloud+ Premier systems and this is included for Naviam Cloud and Cloud+ Enterprise systems.

SCIM Synchronisation

The SCIM Authentication method can be utilised by Customers as an add-on service; this is not a standard, included method. This is available as an add-on for Naviam Cloud and Cloud+ Premier systems and included for Naviam Cloud and Cloud+ Enterprise systems.

Site-to-Site VPN

Enables a secure connection between two networks, allowing data exchange. The standard site-to-site VPN includes 5 hours for setup and 5 annual support hours. This is available as an add-on for Naviam Cloud and Cloud+ Premier systems and is included for Naviam Cloud and Cloud+ Enterprise systems.

S3 or SFTP Site

A site to allow for documents to be uploaded and transferred securely over an encrypted connection as needed. This is available as an add-on for Naviam Cloud and Cloud+ Premier systems, but this is included for Naviam Cloud and Cloud+ Enterprise systems.

Database and Doclinks Growth

Database and Doclinks growth beyond the initially provisioned sizing will be available to Naviam Cloud and Cloud+ Starter, Premier, and Enterprise customers and charged in increment blocks based on the "Naviam Starter, Premier, & Enterprise Feature Table

Backup & Storage Regime

Backup Regime by Platform

The following table shows the backup regime for the DB2, SQL Server, and Oracle database platforms, and is employed within the Cloud Services.

If the Customer does not know which database platform is being used in the solution, please contact technical support or your technical account manager.

Production Database Backups

Frequency of Backups	
Full Daily Backups - frequency	1 Daily
Full Monthly Backups - frequency	1 Monthly
Incremental Backups - frequency	Incremental - Every 12 Hours
Transactional Logs - frequency	Every 15 Minutes
Retention of Backups	
Full Daily Backups - retention	30 Days
Full Monthly Backups - retention	12 Months
Incremental Backups - retention	30 Days
Transaction Logs - retention	30 Days

Non-Production Database Backups (all NPEs)

Frequency of Backups	
Full Daily Backups - frequency	1 Daily
Retention of Backups	
Full Daily Backups - retention	10 Days

Production Attached Documents Backups

Frequency of Backups	
Full Weekly Backups - frequency	1 Weekly
Full Monthly Backups - frequency	1 Monthly
Retention of Backups	
Full Weekly Backups - retention	30 Days
Full Monthly Backups - retention	12 Months

Extended Backup Retention Regime

If there is a customer requirement for an extended retention of database backups, there may be an option for the Customer to be provided backup files from Naviam, but the Customer is responsible for storing these within the Customer network. This would be an additional service requiring additional fees dependent on Customer requirements.

Naviam can also provide Customers with additional storage for database backup retention. Customers should note that each store point would be a distinct file rather than “x” years’ worth of data.



Patching, Change, Upgrade Regime

Patching/Upgrade Cycles for MAS and OpenShift Clusters

Maximo Application Suite requires regular patching to keep all component versions in support with both the product vendors as well as each other.

Patching and maintenance will be performed on hosted customer systems when necessary to maintain versions within vendor support and never without a valid reason or unjustifiably.

Customer MAS Patching/Upgrade Schedule

The Naviam Cloud and Cloud+ patching/upgrade schedule aims to align with the timing of new major version releases and maintenance updates for each major version from IBM. Our current patching/upgrade approach assumes that IBM aims to provide a new major version release every year and maintenance updates for each major version for up to 3 years, but this is subject to change.

Customers on the Naviam Cloud and Cloud+ hosted systems should expect the regular patch cycle for MAS Core & Manage to be around 6–12 months. Where this patching involves minor version upgrades, these involve bug fixes and security fixes rather than Functional Upgrade changes. These upgrades, whilst requiring some regression testing by Customer, do not require the same level of regression testing and upgrade of other solution stack components as major version upgrades.

Within this 6–12-month cycle, approximately every 24 months, the Customer should expect the upgrade to be a major version. This is to remain on a supported version, avoiding the earlier release versions and having time to test and cut over within the supportable window. When a major version upgrade is applied, the Customer should note that some functional changes may result. It is advised that the Customer carry out adequate functional and regression testing in non-production environments (when Naviam upgrades those environments) before this upgrade is applied to Production.

When preparing for a new patch or upgrade, the Customer may incur fees from Naviam for the functional work, code merge, project management, or other functional patch/upgrade project work.

The specific schedule will vary at contract term inception based on where in the patching cycle Customer systems enter the Naviam cloud, but after the first upgrade cycle, the future schedule should be clearer to understand and plan for.

Other elements of the solution stack, such as DB2 and infrastructure components, operate with differing patching cycles.

Patching/upgrade cycles will apply to both shared (SCML Platforms) and dedicated MAS OpenShift clusters (Dedicated Platforms).

Notification

Naviam will inform the Customer that a patching/upgrade cycle on any specific MAS OpenShift cluster is required before a certain date with the following target of notice:

4 Months' notice, where possible, of the need for a routine/regular upcoming patching and/or upgrade cycle to MAS OpenShift clusters.

Prescriptive & Consultative Patch Schedules for OpenShift Clusters

SCML MAS OpenShift platforms (Naviam Cloud and Cloud+ Starter and Premier) carry a prescriptive patching schedule. Dedicated MAS OpenShift clusters (Naviam Cloud and Cloud+ Enterprise) carry a consultative patching schedule.

A *prescriptive patching* schedule means that if the notice periods are followed, the Customer cannot deny or refuse to be patched or upgraded. This is because they are hosted on a shared (SCML) platform, and denial would delay the patching schedule; this could affect other Customers on the platform, potentially causing their systems to go out of support with the vendor.

A *consultative patching* schedule means that Naviam will consult with Customer on when dedicated clusters are to be patched and agree to alternative dates/times if Customer suggests or stipulates them. However, if continued Customer non-acceptance or inability to agree on patching outages with Naviam results in any component within the Cloud or Cloud+ Solution to go End of Support/End of Life with its software vendor, then Naviam reserves the right to:

- suspend the SLA for Incident response and uptime Availability
- suspend any service credits available
- issue a commercial order to Customer which would affect the hosting fees in full or in part (which reflect the risk and additional effort of managing and maintaining a hosted solution without a back-to-back support agreement in place with the vendor); for any time up until the system can be patched back into version/s currently supported by the vendor.
- Customer should also note that for any time that the hosted solution is run outside of vendor support, no security fixes to any published vulnerabilities may be available until the hosted system can be patched back into a vendor-supported version. Details of such commercial orders and their content in these circumstances will be detailed within.

Planned Downtimes per Activity

The following table shows the planned Downtimes that Customers can expect on MAS OpenShift clusters, with estimated Downtimes for each type of activity. Estimated outage times for planned downtimes are intended to take place outside of the Customer's standard business hours or during off-peak hours.

The notification provided to Customers regarding a planned Production outage will be provided to a pre-determined list of Customer stakeholders via email; there will also be visibility into this notification within Naviam Dashboard.

Maintenance	Expected Frequency	Estimated Outage Time	Notification to Customer (Production Outage)
OpenShift Cluster Patch/Upgrade Example: v4.20.x to v4.22. y	Every 12 months	Expected 4-hour outage that can last up to 8 hours	The target is 4 months in advance of the cycle to begin.
MAS and Manage Patch/Upgrade Example: v9.1.x to 9.2.x or v9.1.9 to v9.1.23 Technical Upgrade only	Every 6-12 months and when required by Naviam or requested by Customer	Up to 4 hours	The target is 10 Business Days (if requested by the Customer or required by Naviam) outside of a planned patching/upgrade cycle.
Operating System Patching for Databases	Every 3 months	Up to 1 hour	The target is 10 Business Days in advance
Database Platform Patch/Upgrade	Every 12 months	Up to 4 hours	The target is 10 Business Days (if requested by the Customer or required by Naviam) outside of a planned patching/upgrade cycle.

Maintenance	Expected Frequency	Estimated Outage Time	Notification to Customer (Production Outage)
HIGH security and/or vulnerability patching (for CVSS 7.0 to 9.0 rated vulnerabilities)	When identified in ongoing vulnerability scanning	Up to 4 hours	The patch should be applied to Production no later than 30 calendar days after the first notification
CRITICAL security and/or vulnerability patching (for CVSS 9.0 to 10.0 rated vulnerabilities)	When identified in ongoing vulnerability scanning	Up to 4 hours	The patch should be applied to Production no later than 14 calendar days after the first notification
Failover / Disaster Recovery Testing	Annually - at customer request	Up to 48 hours	The target is 30 Business Days in advance

New Version Release

When a new IBM catalogue is released for general use, Naviam will evaluate it for a minimum of 30 days. Following successful evaluation, Naviam will release the new version for use in the Non-Production Customer system at the Customer's request. After a minimum of 30 days in the Non-Production Environment, Naviam will release the new version for use in the Customer Production system at the Customer's request.

If during the new version testing period issues are identified, Naviam will alert Customers requesting a new version release who may be affected by the issue(s).

Patching Outage Timings

Each Planned Downtime outage will be arranged with the Customer but will be within the generic time stated below:

Planned Downtime Default Period: 18:00 to 06:00 in Customer Default Time Zone, weekdays only (not weekends).

iFixes, Hotfixes and LA Fixes

The application of iFixes, Hotfixes and LA fixes when they are required is a fully inclusive element of the Cloud Services provided by Naviam.

Fixes will only be applied if a core or inherent bug or issue has been identified in the Application Layer, for which the vendor has released an iFix that addresses that specific issue, and for which a fix item has been included in the build release notes for that iFix. There is no limit to the number of fixes which can be applied as an inclusive element to the Cloud Services if this criterion is met.

Security Vulnerability Fixes

Naviam commits to applying all or any security fixes or patches to hosted solutions within a specifically defined timescale to address vulnerabilities that, upon assessment, could impact the Cloud Services, or Naviam's ability to provide the Cloud Services in part or in full. These special timescales apply to *HIGH and CRITICAL identified security vulnerabilities using the CVSS (Common Vulnerability Scoring System v3 -below), and for which patches have been released by the vendor responsible.

Severity	Score	Description
Critical	9.0 - 10.0	Exploitation is straightforward or well-known and exploits usually result in system-level compromise
High	7.0 - 8.9	Exploitation is more difficult or less well known but could result in elevated privileges and potential loss of data or downtime
Medium	4.0 - 6.9	Vulnerabilities exist but cannot be exploited, however with extra steps such as additional social engineering, bad actors could gain some level of interactive control or data access
Low	0.1 - 3.9	Vulnerabilities are non-exploitable but bad actors could use them to reduce an organisation's attack surface or learn more about the system to facilitate onwards attacks

Info	0	Information only risk for bad actors
------	---	--------------------------------------

The following table illustrates the pre-determined timescales defined for the application of all or any required patches/updates to address HIGH and CRITICAL vulnerabilities:

Patching Type	Initial Notification	To NPE 1 application	To Production application (Maximum Target to Production)
HIGH Vulnerability Patch/Upgrade (CVSS 7.0-8.9)	0 days [1]	12 days	30 days [4] [5]
CRITICAL Vulnerability Patch/Upgrade (CVSS 9-10)	0 days [1]	5 days [2] [3]	14 days [4] [6]

Notes:

[1] The timescale for application to Production for either severity starts at the first notification to Solution Provider – this is day 0 in the timescale.

[2] CRITICAL severity patches will be applied to NPE1 within 5 days of initial notification – so 5 days after day 0. Solution Provider will be given the opportunity to regression test this patch/upgrade from this point to the point at which the patch/upgrade is applied to Production.

[3] CRITICAL severity patches will be applied to NPE1 first due to the short timescale in which the patch/upgrade needs to be applied – this means that the Solution Provider will only be given the chance to regression test in one Non-Production Environment before application of the patch/upgrade to Production.

[4] Any other Non-Production Environments will be backfilled after application to Production.

[5] Target to apply HIGH severity patches to Production: 30 days from day 0 (initial notification)

[6] Target to apply CRITICAL severity patches to Production: 30 days from day 0 (initial notification)

Service Level Agreement

The Service Level Agreement (SLA) contains information on the Naviam Cloud and Cloud+ service commitments, availability commitments, and available SLA Credits. This SLA outlines the general terms and conditions under which Naviam provides certain Cloud Services to the Customer. Notwithstanding anything to the contrary in this SLA or otherwise, this SLA does not apply to services for any Non-Production and Demo instance. Any systems still undergoing implementation are not subject to this SLA until all implementation activities are complete.

Component Availability

Non-Production Application Availability

Non-Production and demo systems are architected for the same levels of high Availability as Production Environments. Due to shared administrative access, Non-Production Availability is provided on a best-efforts basis.

Integration Availability

Integrations are dependent on the Availability of the external systems being integrated, as well as other supporting networking configurations required to secure those communications. Naviam recommends the use of the Maximo REST API for inbound integrations into Maximo. This integration method into Maximo is supported by the Service Level Agreement. Other types of integrations and endpoints are supported on a best-efforts basis and are not subject to the application Service Level Agreement.

Mobile Application Availability

Mobile applications serviced alongside the Naviam Cloud and Cloud+ solution may or may not be subject to the Service Level Agreement. If the mobile application connects to Maximo over REST API, that connectivity is subject to the Service Level Agreement. Other mobile application Availability is provided on a best-efforts basis.

Naviam Mobile Availability commitments are covered by the "Service Level Agreement Table".

Application Authentication Availability

The SAML and Local (Native) authentication methods are subject to the Service Level Agreement.

Availability Terms

Availability commitments are described in the “Service Level Table” section below. Availability commitments are provided for hardware, network, and software applications for Production solutions hosted by Naviam. No Availability commitment is provided for Maximo embedded solution components hosted in the Customer computing environment.

The Customer must be able to access the Naviam resources to which they have subscribed. Naviam data centres are designed and engineered to meet the requirements of ISO 27001, ISO 27017, and Service Organisation Control (SOC). Availability is determined based on 24 hours per day and 7 days per week, except for times of unavailability due to planned Downtime exclusions such as:

(i) planned maintenance windows for which Naviam provides at least 7 days prior notice; (ii) failure of any network or internet infrastructure not owned or managed by Naviam; (iii) Downtime caused by any failure of Customer’s computer systems, network, hardware or software or its telecommunications equipment or other equipment; (iv) Downtime caused by any act or omission of any End-User that is inconsistent with Naviam’s suggested use or Customer’s authorized use of the system; (v) Downtime caused by events beyond Naviam’s reasonable control; (vi) Mitigation activities that relate to a critically high vulnerability.

Naviam Cloud and Cloud+ Standard Solution Set SLA

This section outlines the general terms and conditions under which Naviam provides the Cloud Services to the Customer. The “Service Level Agreement Table” is applicable to components in the Naviam Cloud and Cloud+ solution set, unless otherwise specified.

The following table shows the Service Level Agreement between Naviam and the Customer:

Service Level Agreement Table			
Monthly Availability Targets			
	Naviam Starter	Naviam Premier	Naviam Enterprise
SLA	99.95%	99.95%	99.99%
Recovery Time Objective and Recovery Point Objective (Standard Offering)			
	Naviam Starter	Naviam Premier	Naviam Enterprise
RTO	72 Hours	24 Hours	16 Hours
RPO	2 Hours	2 Hours	1 Hours
Recovery Time Objective and Recovery Point Objective (Enhanced Offering)			
	Naviam Starter	Naviam Premier	Naviam Enterprise
RTO	Not Available	16 Hours	Contact Sales for Details
RPO	Not Available	1 Hour	Contact Sales for Details

Naviam Response Commitment & Product-Specific SLA

Naviam response commitments and product-specific commitments are documented within the Naviam Product Descriptions and Support Commitment documents, which can be found here: customers.naviam.io

Naviam Hosted Product SLA

The Naviam products requiring hosted components will follow the Service Level Agreement table above when the hosted components of the solution are provided by Naviam.

For Naviam products not hosted by Naviam, the Service Level Agreement Table above is not applicable.

Service Credits

Service Credits are available for Naviam Starter, Premier and Enterprise where monthly Availability falls below the agreed upon limits.

All or any Service Credits issued under this scheme will only take the form of credits to be applied to upcoming annual recurring fees only and will be calculated to be an amount subtracted from the upcoming renewal fee. Service Credits are calculated and reported based on a calendar months Availability. Service Credits under this scheme have no monetary value outside of an amount to be subtracted from the upcoming renewal fee. Any days prior to the use of the service will be calculated to have had 100% Availability.

Elements of Service Covered by the Service Credit Scheme

The only element of service covered by the Service Credit Scheme is the Availability target for the Naviam Cloud and Cloud+ standard solution set. This is measured on a calendar month basis.

Service Credits can be claimed for monthly Availability below 99.95% (where the offering has a 99.95% Availability target per month) and for monthly Availability below 99.99% (where the offering has a 99.99% Availability target per month). Refer to the SLA table above for the availability targets set for the different offerings.

99.95% Availability Target

For Naviam Starter and Premier systems, the Naviam Cloud and Cloud+ standard solution set carries a 99.95% Availability target (unless otherwise specified); the table below shows how the Service Level Credit amount will be calculated. Service Level Credits may be applied only as a credit to the next upcoming anniversary or renewal fee.

Monthly SLA Credit Table – 99.95% Availability Target

Availability per Month From	Availability per Month To	Monthly Service Level Credit which can be claimed
99.94%	99.90%	2% of service Fees Calculated Monthly Pro-rata
99.89%	99.00%	5% of service Fees Calculated Monthly Pro-rata
98.99%	95.00%	10% of service Fees Calculated Monthly Pro-rata
94.99% or Lower		20% of service Fees Calculated Monthly Pro-rata

99.99% Availability Target

For Naviam Enterprise systems, the Naviam Cloud and Cloud+ standard solution set carries a 99.99% Availability target (unless otherwise specified); the table below shows how the Service Level Credit amount will be calculated. Service Level Credits may be applied only as a credit to the next upcoming anniversary or renewal fee.

Monthly SLA Credit Table – 99.99% Availability Target

Availability per Month From	Availability per Month To	Monthly Service Level Credit which can be claimed
99.98%	99.90%	3% of service Fees Calculated Monthly Pro-rata
99.89%	99.00%	6% of service Fees Calculated Monthly Pro-rata
98.99%	95.00%	12% of service Fees Calculated Monthly Pro-rata
94.99% or Lower		20% of service Fees Calculated Monthly Pro-rata

Claiming Service Level Credits

Service Level Credits must be requested in writing via the submission of a service request to Naviam within one month following the affected month. The Customer will always be responsible for submitting claims to receive Service Level Credits.

Change Freeze Periods

Change freeze periods occur during periods of the year when resources may be limited, and system stability is critical. Change freeze periods apply to any change that could result in scheduled or unscheduled downtime for a Production system. Production changes will be deferred during this period unless explicitly reviewed and approved by Naviam.

In general, the global annual end-of-year change freeze period includes the last two full weeks of December and the first full week of January. The specific timeline for the global end-of-year change freeze period will be communicated in advance with the Customer. Any region-specific change freeze windows will be communicated in advance with the Customer with at least 45 days' notice.

Appendix A – Naviam Software Solutions

Naviam Cloud+ Premier includes a suite of exclusive software solutions that give our customers a clear advantage. Designed, developed, and supported directly by Naviam, these tools deliver enhanced capabilities

While others rely on custom code or third-party add-ons, Naviam provides integrated, upgrade-safe applications that streamline work, reduce effort, and enhance usability without added complexity or technical debt.

The Naviam Elevate Suite, Naviam Accelerators, Naviam Mobile Solutions, Naviam Datastudio, Naviam Planner, and Naviam GIS create a unified toolkit that improves efficiency, strengthens insight, and modernises how your teams operate. Every solution remains compatible with new Maximo releases and is automatically delivered to Naviam Cloud+ customers, with no effort required from the Buyer

You stay focused on performance while Naviam delivers software that makes your work faster, easier, and uniquely powerful.

Naviam Elevate Suite

Data Management for Maximo

The Naviam Elevate Suite is included with Naviam Cloud+. It provides a powerful collection of applications, enhancements, and administrative tools designed to help both end users and system administrators work faster and more efficiently. These capabilities streamline key processes, reduce manual effort, and make Maximo easier to use across your entire organization.

The Elevate Suite is built in as standard and can be enabled for the buyer as required. It is fully supported by Naviam and continuously updated to remain compatible with all new Maximo versions. New features and enhancements are released on an ongoing basis and automatically delivered to Naviam Cloud+ customers, ensuring you always benefit from the latest improvements without upgrades or extra configuration.

The Elevate Suite currently includes the following functions.

Function	Description
Rentals	A simplified application based on Item Master that lets users quickly add rental items and make them available for Work Orders.
Job Plan Lock on Use	Adds a new flag to Job Plans that prevents changes to planned materials, services, tools, labour, or tasks once they are added to a Work Order.
Flex Calendar	A comprehensive, drag-and-drop calendar view that visualizes work orders, downtime, and preventive maintenance to support easier scheduling and planning.
Work Order Purchasing Summary	A consolidated view within the Work Order application showing all related purchase requisitions, purchase orders, and spending details in one place.
Safety Bulletins	Allows creation and management of safety bulletins, including associated actions, messages, and required measures.
Planned Material to Purchase Requisition Fields	Allows selected fields to be automatically copied from Planned Materials into Purchase Requisitions.
Quality Audit (Work Orders)	Enables creation of quality audits by defining criteria and selecting either a specific number or percentage of work orders, with filters for assets, job plans, PMs, priorities, and more.
User Profile Delegates	Adds delegate and date range fields to user profiles. Assignments are automatically routed to the designated user, ideal for holiday or sickness cover.

Function	Description
Repairs Process	A simplified application and process for repairing items and assets with unnecessary fields removed and the layout optimized for ease of use.
Show Attachments	Allows quick viewing of images, PDFs, and other files via a streamlined viewer, without opening each attachment individually.
Gallery Tab	Adds a gallery-style tab across all Maximo applications that displays attachments, such as images, PDFs, and text files, stored locally or in the cloud.
Email Listener	Allows attachments to be added to any record by emailing them to a monitored mailbox, with full tracking of each attachment's origin.
Download All Attachments	Adds a button that zips all attachments on a record and downloads them as a single file bundle.
Drag and Drop Attachments	Enhances the standard attachment workflow by allowing files to be added simply by dragging them into the attachment area.
SharePoint Adapter	Enables direct printing of attachments stored in SharePoint using configuration and automation scripts without custom code.

Administrative Functions

Function	Description
Admin Toolbox	Enhancements to admin applications, such as Security Groups and Database Configuration, to improve usability and efficiency.
E-Audit Table Generation	Adds a one-click option in Database Configuration that automatically generates all required audit tables.
Copy Person Groups Dialog	Allows quick duplication of Person Groups, saving time and avoiding re-creation from scratch.
Workflow App Enhancements	Adds new filterable columns in the Workflow Admin application for Invoice, PR, PO, Work Order, and Company numbers to make workflow searches faster and easier.
Query Enhancements	Introduces a central Query Manager to manage queries, see where they are used on Start Centres, and adjust query clauses. Also includes group-based query access restrictions.
People App Person Groups	Adds a tab in the People application that displays associated Person Groups for quicker reference.
People App Auto-Sequencing	Corrects sequencing issues in the Person Groups tab of the People application.
Off-Boarding Workflow	Automates user offboarding by reassigning owned records to a replacement user to prevent orphaned data.

Naviam Mobile Solutions

Extend Maximo to the Field with Powerful Mobile

Mobile work management solutions offer substantial advantages by providing engineers with essential information to safely perform their duties, while also facilitating accurate and efficient documentation of inspections and failure reports.

Naviam Mobile Solutions extends the power of Maximo into the field through three purpose-built applications: Opqo, EZMaxMobile, and Fingertip. Each solution is designed for enterprise operations and delivers secure, reliable mobile access to the work, assets, and data your teams depend on. With real-time and offline capability, intuitive workflows, and seamless integration with Naviam Cloud+, these mobile tools help technicians and field staff work faster, capture accurate information, and maintain consistent performance across even the most distributed environments.

These solutions are described in more detail in the Appendix B

Naviam Datastudio

Data Management for Maximo

Naviam DataStudio is a web-based data management tool for IBM Maximo that allows teams to query, edit, validate, and upload large datasets with accuracy and control. A real-time validation engine ensures that all updates follow Maximo rules and standards before being approved through workflow and committed to the system. With secure role-based access, workflow-driven approvals, and all data stored inside Maximo, DataStudio helps organizations onboard assets, standardize records, and complete data-driven projects faster and with greater confidence.

Key Highlights

- Streamlines bulk data creation and updates using templates and guided tools
- Validates data in real time to enforce formats, values, and Maximo business rules
- Enables secure, role-based collaboration without external data storage
- Uses Maximo's native security and workflow for approvals and governance
- Speeds up data onboarding, cleanup, and migration projects

- Provides bulk upload and export capabilities for efficient operations
- Includes visual feedback and error navigation to correct issues quickly



Appendix B – Naviam Mobile Solutions

Naviam Mobile Solutions extends the power of Maximo into the field through three purpose-built applications: Opqo, EZMaxMobile, and Fingertip. Each solution is designed for enterprise operations and delivers secure, reliable mobile access to the work, assets, and data your teams depend on. With real-time and offline capability, intuitive workflows, and seamless integration with Naviam Cloud+, these mobile tools help technicians and field staff work faster, capture accurate information, and maintain consistent performance across even the most distributed environments.

Opqo by Naviam

Opqo is a clean, efficient mobile app for IBM Maximo that is simple to purchase, configure, and deploy. With no server installation or upfront project required, organizations can get started in minutes. Opqo supports both online and offline work, integrates directly with Maximo's existing workflows and security model, and is available on the Apple App Store and Google Play.

Key Highlights

- Zero upfront commitments with a free trial option
- Instant setup by entering Maximo connection details
- Configurable entirely within Maximo using existing workflows
- Fully operational offline with automatic syncing
- Modular, process-led interface for focused user screens
- Native iOS and Android support for phones and tablets
- Robust field functionality, including work orders, inspections, timekeeping, and meter readings
- Mobile inventory tools for issuing, transfers, returns, cycle counts, and barcode or QR scanning
- Asset data capture using Maximo-defined forms
- Secure REST API integration with no middleware required
- Easy enterprise rollout through DNS auto-discovery, QR setup, and MDM support
- Proven fast deployments with successful proofs of concept completed in under one month

EZMaxMobile by Naviam

EZMaxMobile is a comprehensive mobile solution for IBM Maximo that keeps field teams connected and productive, no matter where they are. It provides real-time communication, robust offline capability, and complete adherence to Maximo's security settings and business rules. The app is device-agnostic, supports all major MDM platforms, integrates with ArcGIS and Maximo Inspection Forms, and enables field users to capture photos, scan barcodes, record time, complete workflows, and access reports across 24 languages. Designed for both simple and complex deployments, EZMaxMobile helps organizations streamline field operations, improve efficiency, and modernize their Maximo mobile experience.

Key Highlights

- Supports 25 or more Maximo processes, including work orders, assets, inspections, and inventory
- Engineered for multi-day or weeklong offline work with fast syncing and local caching
- Adheres to all existing and new Maximo business rules without reconfiguration
- Offers rich device functionality, including photos, videos, barcode scanning, signatures, and push notifications
- Device-agnostic mobile app available on iOS, Android, and Windows via app stores or MDM distribution
- Responsive UI designed for phones, tablets, and rugged devices
- Built for large and complex environments with 100–200 or more field users
- Work order and asset management with real-time updates
- Inventory and supply chain capabilities, including material tracking and issuing
- Offline mode with automatic sync when reconnected
- Customizable workflows, screens, and fields to match operational needs
- Integrated ESRI mapping to visualize Maximo data, navigate to assets, and create records from the map

Fingertip by Naviam

Fingertip is a highly configurable mobile solution for IBM Maximo that delivers essential maintenance, inventory, and asset functionality directly to field users on iOS, Android, and Windows devices. Built for rapid deployment and optimized for real-world environments, it requires no custom development or additional infrastructure. Fingertip combines offline-first capabilities, barcode and NFC scanning, ArcGIS integration, push notifications, and flexible mobile forms to help organizations streamline field operations, reduce IT overhead, and quickly and cost-effectively extend Maximo to the workforce.

Key Highlights

- Configurable within Maximo using built-in tools and no-code logic
- Offline-first architecture with fast delta syncing and reliable field performance
- Powerful mobile forms with conditional logic and workflow support
- No additional infrastructure required and no middleware to maintain
- Fast deployment using existing Maximo skills and configurations
- Supports multiple modules such as Work Orders, Calibration, Inventory, Assets, Supply Chain, and Service Requests
- Mobile access to core Maximo functions, including work updates and inventory transactions
- Role-based access through Maximo Security Groups
- Integrated barcode, NFC, and QR scanning
- Built-in ArcGIS integration for geospatial visibility and asset context

Naviam's Cloud and SaaS support services provide essential and enhanced assistance to all our direct customers, covering both product software solutions and related services. Our core focus centres on hosted and managed IBM Maximo Enterprise Asset Management platforms, as well as Naviam's range of products and software designed to optimise the functionality of the core platform. Our support offering, prioritising effective issue management, prompt responsiveness, and sound escalation procedures recognising the business criticality of this system.

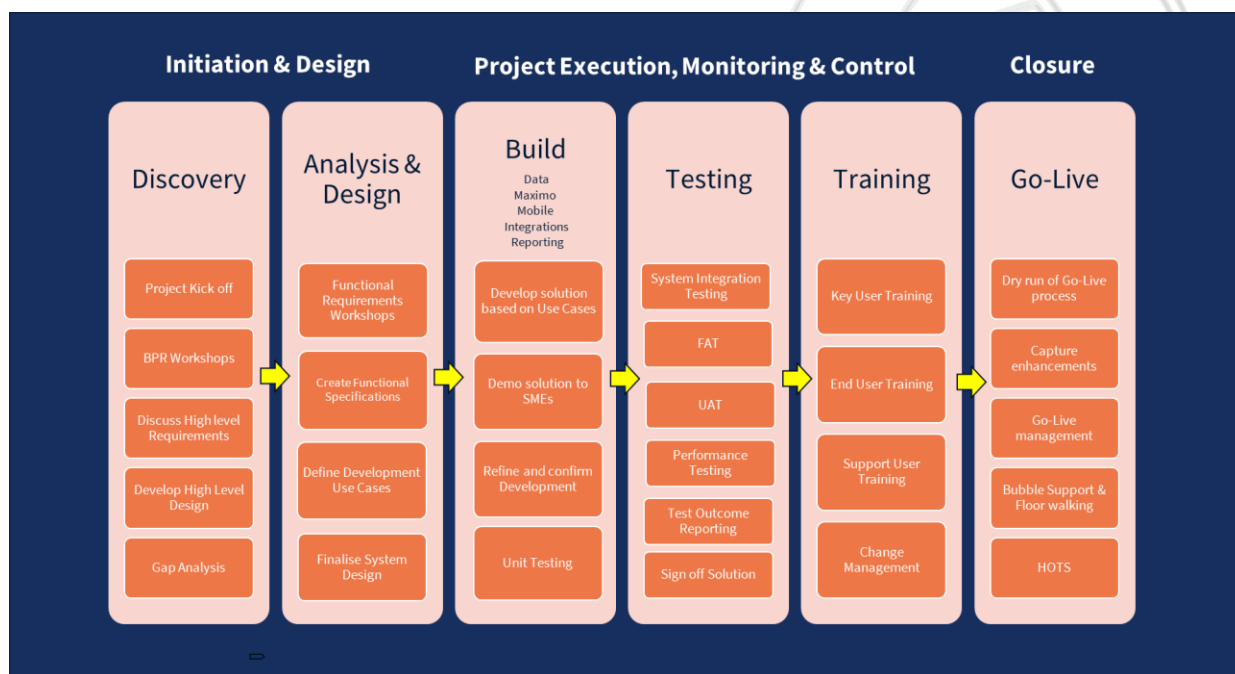
Naviam's Cloud and SaaS support delivers fast, effective assistance for IBM Maximo EAM and Naviam products, with robust issue management and escalation. Our team maintains

business-critical systems, optimises Maximo's hosted, managed platforms, and provides responsive and knowledgeable support for all direct customers, helping them maximise system value.

Appendix C Project Implementation Approach

Implementation Methodology

Below is the Naviam project lifecycle process. Each project stage describes the expected documentation and deliverables. This process is designed to be flexible to fit in with any specific requirements the client may have.



Stage 1 – Discovery

Stage Objectives: *To define the 'Project Delivery Plan', to establish and agree the Business Processes, to agree and design the required IT landscape and to provision all required Project Environments.*

Key Activities:

- PM will conduct Project Initiation 'Kick-off' meeting(s) with all key stakeholders and appropriate SME's.
- Provide the 'Project Delivery Plan'
- Using process modelling techniques, the Design Authority team will conduct BPR Workshops to cover each key Business Process (including Interface and Reporting needs).
- Infrastructure teams agree IT Environment requirements (to including all Infosec needs)
- Build the agreed IT Environments.

Outputs:

- Fully documented 'Project Charter' to include the following:-
 - Agreed Project Scope.
 - Approach for Risk, Issues and Change Management.
 - Key Resources and Contact Details.
 - Team Structure and Escalations Process.
 - Communications Protocols.
 - Approvals mechanisms and timings.
 - Testing Approach (including entry and exit criteria).
 - Training Approach.
- Documented and approved Business Process maps that will form the basis against which the system is designed.
- Documented and approved IT Landscape requirements.
- Project Environments built and ready for use.

Stage 2 – Analysis & Design

Stage Objectives: *To establish the Functional Requirements, define the fully integrated 'System Design' and to establish the supporting Data Definition requirements.*

Key Activities:

- Using the BPR outputs from the Discovery Phase the Design Authority team will conduct a series of 'Functional Requirements' definition workshops. (these will also include the establishment of the Interface and Reporting needs).
- Informed by these 'FRS' workshops, the Infrastructure team will define the overall 'System Architecture'.
- Likewise, using information coming out of the FRS workshops, the Data Team will define all the Data Definitions needed to support the overall System Design.

Outputs:

- A suite of fully documented 'Functional Requirements Specifications' (FRS's) that will form the basis of the 'Build' phase.
- Documented Integration requirements.
- Documented Reporting requirements.
- Fully documented System Architecture.
- Documented Data Definitions.
- 'Quality Gate Approval' of the 'MaxiCloud' solution design.

Stage 3 – Build

Stage Objectives: *To develop the Functional, Integration and Reporting Requirement into a fully functioning, Integrated solution ready to handover for System Integration Testing.*

Key Activities:

- Using the approved FRSS as the baseline, create a full suite of Azure DevOps 'Use Cases'. These will provide the basis for the product development, testing and training needs.
- Using 'Fast-track' methodology, based on these use cases, define and conduct several development 'packages'
- Conduct in-package Unit Testing.
- In parallel, [Naviam's](#) Data Team will assist with developing and loading the supporting data.

Outputs:

- A fully Configured/Developed system ready for SIT.
- Fully developed Integrations to all peripheral systems (Phase 2).
- Fully developed Reporting solutions.
- Fully defined and loaded Data set.
- **'Quality Gate Approval' of the [MaxiCloud](#) solution build verified as 'Ready for Testing'.**

Stage 4 – Testing

Stage Objectives: *To create SIT Test Cases and execute SIT, support the client through UAT, undertake Performance Testing. Provide 'Test Outcome' reports indicating when the exit criteria has been met.*

Key Activities:

- Phase 1 testing will focus on 'Out of the Box' MAS9 & O&G Accelerator testing. However, for Phase 2 testing NAVIAM's Test Team will create the 'System Integration Test' scripts needed to validate the Phase 2 build deliveries.
- Post the Build Sign-off, conduct the execution of E2E SIT (normally this entails a minimum of 2 x test cycles, with issue resolution period following cycle 1).
- Prepare SIT outcome reports.
- Provide support during the client's execution of UAT (2 x cycles with issue resolution periods in between).

Outputs:

- Fully defined set of manual SIT test cases.
- SIT test outcome reports for all SIT cycles.
- Sign-off of SIT (i.e. once defined exit criteria has been met).
- UAT Test outcome reports for all cycles (client responsibility).
- Sign-off of UAT (i.e. once defined exit criteria has been met).
- **'Quality Gate Approval' of the [MaxiCloud](#) solution to be verified as 'Ready for Production Release'.**

Stage 5 – Training

Objectives: *To conduct the Training Needs Analysis, to create Training Material, to provide the 'Super-User' training ahead of UAT.*

Key Activities:

- Training needs analysis is completed, and the decision made around how it will be delivered.
- Informed by the development 'Use Cases' and where appropriate create bespoke training material to support training delivery.
- Deliver training to the clients 'Super-Users' ahead of their execution of UAT.

Outputs:

- Full set of Training Material available in the agreed format(s).
- Super-Users are now properly equipped with the knowledge required to successfully conduct UAT.
- The THREE60 Trainer is suitably equipped to deliver training to the THREE60 end user community.

Stage 6 – Go-Live

Stage Objectives: *To perform a number of Go-Live 'Dress Rehearsals', Execute all Go-Live activities, perform post Go-Live 'Smoke Tests' and hand over the System to Operations.*

Key Activities:

- Create the Initial Cut-Over 'Run Book'.
- Work with all relevant parties to perform a timed 'Dress Rehearsal'.
- Collate findings and update Run Book accordingly.
- Re-run Dress Rehearsal as needed until all activities execute without issue.
- Clear down any test data and then perform Go-Live for real'
- Conduct System Verification 'Smoke Tests'
- Hand system over for Operational usage.

Outputs:

- Fully documented 'Run-Book' to facilitate Go-Live cutover.
- Signed of system verification
- **'Quality Gate Approval' of the MaxiCloud solution to be verified as 'Operational' (i.e., live in Production).**

Post Go-Live

Post Go-Live Activities: *To handover the system to the BAU support team and in parallel, for project 'Hypercare' period to commence.*

Key Activities:

- Conduct any final updates to the 'As-Built' documentation,
- Complete any outstanding 'Knowledge Transfer' to support personnel.
- Conduct completion of all required BAU support documentation.
- Provide focused 'Hypercare' support though the agreed time period

Outputs:

- Provide fully updated 'As-Built' Functional Specifications.
- Provide fully completed BAU support documentation.
- Limited project personnel remain available to provide the agreed Hypercare support.

Project Closure

Key Activities: *Notify and obtain customer acceptance of the project delivery, assess project performance and lessons learned. Close commercial aspects of the project.*

- Project completion certificate signed – off.
- Customer satisfaction assessment issued (PM/PMO).
- Request for customer testimonial and case study (where appropriate).
- Finalise billings and obtain final payments.
- Review project performance, analyse lessons learned. Update NAVIAM's internal repositories.
- Closure of project and WBS lines in all systems.
- Support team takes over BAU responsibilities.

